

Generieke actielijst klantcontact met privacygevoelige, juridische en financiële informatie

Inleiding

Bibliotheken spelen een actieve rol in het sociale domein en breiden hun dienstverlening steeds meer uit. Denk bijvoorbeeld aan het convenant dat de Koninklijke Bibliotheek in 2016 met de Belastingdienst heeft afgesloten. De medewerkers met klantcontacten ('in de frontoffice') worden daardoor steeds vaker geconfronteerd met hulpvragen waarbij privacy-aspecten en gevoelige financiële informatie een rol spelen.

Het is belangrijk dat de Bibliotheek hier goed op voorbereid is en hierover afspraken maakt met het frontoffice-personeel. Zo hoeven medewerkers niet zelf te bepalen hoe ver ze gaan in het helpen van de klant en vermijdt de Bibliotheek onnodige risico's.

Om de medewerker goed toe te rusten om te werken binnen de werkafspraken en het gewenste niveau van dienstverlening te bieden en op de juiste manier, moet de Bibliotheek een aantal randvoorwaarden realiseren. Dit document is bedoeld als actielijst om deze randvoorwaarden te regelen. Het geeft een opsomming van zaken die voor elke medewerker helder en toegankelijk omschreven moeten zijn.

De bibliotheekrealiteit zal door maatschappelijke en technische ontwikkelingen blijven veranderen. De actielijst is daarom geen statisch document. Het wordt waar nodig aangepast en is afhankelijk van de situatie in de lokale Bibliotheek.

Bijsluiter

Achtergrond bij de generieke actielijst

De actielijst is ontwikkeld binnen het ProBiblio-project 'Privacy in de frontoffice'. Het doel van het project is om Bibliotheken te helpen bij het bepalen van de grenzen in hun dienstverlening. Samen met medewerkers en leidinggevenden zoeken de adviseurs in een (of meer) sessie(s) de gewenste werkwijze voor de Bibliotheek. De uitkomst van dat proces wordt vastgelegd in een medewerkersprotocol. Hierin staan de afspraken over hoe de medewerkers in specifieke situaties dienen te handelen. Om er voor te zorgen dat de medewerkers ook daadwerkelijk met het protocol aan de slag kunnen, dient een aantal voorwaardelijke zaken geregeld te zijn. Welke zaken dit zijn wordt opgesomd in de actielijst.

In die projectaanpak is de vastlegging van de afspraken in het protocol en de actielijst dus heel bewust het sluitstuk van een gezamenlijk proces, dat bestaat uit een reeks gesprekken, casebehandelingen en kennisoverdracht. Die aanpak leidt ertoe dat de afspraken meer begrepen en gedragen zijn door alle betrokkenen, en heel concreet aansluiten bij de dagelijkse praktijk. Deze projectaanpak ontbreekt voor het generieke protocol en actielijst. Het generieke protocol en de actielijst worden verstrekt als onderdeel van de toolkit voor Bibliotheken ter ondersteuning van hun activiteiten voor het convenant tussen de Koninklijke Bibliotheek en de Belastingdienst. De inbedding in de organisatie vanuit een voorafgaand proces ontbreekt dus. Deze inbedding zal door de Bibliotheek op een andere manier vorm moeten krijgen. Ook de actielijst zal (gedeeltelijk) uitgevoerd moeten worden, om de medewerkers de tools in handen te geven waarmee ze het protocol ook daadwerkelijk kunnen uitvoeren. Zonder gerichte aandacht hiervoor is het risico groot dat de afspraken in de la belanden, of in de praktijk niet uitgevoerd kunnen worden en het protocol en de actielijst niet bijdragen aan het gewenste resultaat.

Per bibliotheek zullen de documenten een verschillende uitwerking kennen, afhankelijk van de lokale situatie en keuzes!

Inhoud van de actielijst

In het ProBiblio-project 'Privacy in de frontoffice' leidt het proces tot een bewuste en expliciete keuze voor een werkwijze; een bepaald niveau van dienstverlening. We onderscheiden er vijf. Van niets doen tot het de klant volledig uit handen nemen. Bij elke werkwijze geldt feitelijk een set werkafspraken en een bijbehorend protocol.

Zonder het bijbehorende proces te doorlopen heeft een expliciete keuze voor een werkwijze beperkt effect voor de medewerkers in de praktijk. Het is ook niet noodzakelijk om die expliciete keuze te maken. Voor een goed gebruik van het generiek protocol is het wel van belang de achtergrond te begrijpen.

Het voorliggend generiek protocol is ontwikkeld binnen het project 'Privacy in de Frontoffice' met als uitgangspunt werkwijze 2, met in uitzonderingssituaties werkwijze 3.

**De medewerker helpt de klant tot aan het inloggen (= werkwijze 2).
Bij uitzondering – bij bibliotheekeigen producten, technische problemen van bibliotheekapparatuur en tijdens digitale gesprekken – is het de medewerker toegestaan ook na het inloggen mee te kijken met de klant. De medewerker voert echter geen handelingen uit voor de klant (= werkwijze 3).**

We hebben voor deze werkwijze gekozen omdat hierbij de risico's beperkter zijn, omdat de medewerker in deze situatie niet meekijkt bij het inloggen, behalve bij bibliotheekeigen producten. Bovendien kozen tot nu toe de meeste bibliotheken voor deze variant.

De actielijst komt ook voort uit de keuze voor werkwijze 2, maar is in principe ook voor de andere werkwijzen bruikbaar, omdat in de actielijst punten staan die voor elke werkwijze zullen gelden.

Gebruik van de Actielijst

De actielijst beoogt niet volledig te zijn en moet per Bibliotheek specifiek worden gemaakt. Dat houdt in dat degenen die de stukken voor de Bibliotheek toepasbaar maken, moeten nagaan of de genoemde punten goed aansluiten bij de eigen organisatie. Aanpassingen kunnen nodig zijn, afhankelijk van bijvoorbeeld de organisatie (missie en visie, dienstverleningsniveau), locaties, inrichting van de locaties, bezoekersgroepen en hun specifieke wensen en andere karakteristieken, werkafspraken met gemeente, samenwerkingsafspraken en de partners. De actielijst biedt daarom met name een handvat om de aspecten (randvoorwaarden) na te gaan en om eventueel de acties te bepalen om de randvoorwaarden te vervullen.

Ten slotte nog het volgende. De bibliotheekrealiteit zal door maatschappelijke en technische ontwikkelingen blijven veranderen. Zowel het generieke protocol als de actielijst zijn daarom geen statische documenten. Ze worden waar en wanneer nodig aangepast, en daarom verdient het aanbeveling om daarvoor iemand in de organisatie verantwoordelijk te maken.

Overige documenten in de toolkit

- Generiek Protocol
- Generiek Hoofdpunten Protocol

Voor meer informatie

ProBiblio

Laurens Goudriaan, tel. 023 55 46 100, e-mail lgoudriaan@probiblio.nl

Edo Postma, tel. 023 55 46 100, e-mail epostma@probiblio.nl

Bent u geïnteresseerd in het organiseren van het 'Privacy in de frontoffice-traject', neem dan contact op met uw provinciale ondersteuningsinstelling (POI). Deze kan u vertellen wat de mogelijkheden voor uw bibliotheek zijn.

Inhoud

| | |
|--|---|
| Inleiding | 1 |
| Sociale kaart voor doorverwijzen | 4 |
| Externe organisaties | 4 |
| Eigen aanbod | 4 |
| Techniek en inrichting | 5 |
| Publiekswerkplekken; techniek | 5 |
| Publiekswerkplekken; inrichting en privacy | 5 |
| Personeelswerkplekken | 6 |
| Communicatie | 7 |
| Kennis | 8 |
| Overig | 8 |

Sociale kaart voor doorverwijzen

Frontoffice-medewerkers moeten in staat zijn om klanten effectief door te verwijzen en toevallige individuele kennis overstijgen. Daarom is het belangrijk om een overzicht van doorverwijsadressen en eigen activiteiten te hebben. Dit overzicht biedt tevens de mogelijkheid om te inventariseren wat er al is en wat nog mist in het sociale vangnet.

Externe organisaties

Inventariseer het volgende in uw werkgebied:

- De instanties die mensen doorsturen naar de Bibliotheek (banken, UWV, gemeente, Belastingdienst, maatschappelijke instanties etcetera).
 - Wat doen deze instanties wel en wat niet?
 - Waarom worden mensen doorgestuurd?
 - Weten zij wat de Bibliotheek doet?
 - Voor welke vragen kunnen zij klanten doorverwijzen naar de Bibliotheek?
- De diensten en instanties waarover hulpvragen worden gesteld bij de balie. Inventariseer deze bij de frontoffice-medewerkers.
- De instanties die mensen ondersteunen bij zaken doen met financiële, privacygevoelige en persoonlijke aspecten (ouderenbonden, sociaal raadsheren, wetswinkels, Seniorweb, wijkverenigingen, cursusbureaus, etcetera).
 - Bij welke vragen ondersteunen deze organisaties?
 - Wat doen deze instanties wel en wat niet?
 - Wanneer zijn ze open?
 - Weten zij wat de Bibliotheek doet?
 - Hebben de organisaties flyers of posters?
- Wellicht heeft de gemeente al een sociale kaart samengesteld.

Resultaat

Maak een duidelijk overzicht en zorg dat dit centraal beschikbaar komt, bruikbaar voor elke frontoffice-medewerker. Leg flyers neer en hang posters op voor de klanten.

Tip

Ga bij deze instanties langs of nodig ze uit voor een gesprek. Bekijk of er samenwerkingsmogelijkheden zijn. Kunnen zij bijvoorbeeld een cursus, een voorlichtingsavond of wekelijks spreekuur verzorgen in de Bibliotheek? Andere mogelijkheden: oefenomgeving, screenshots van online omgevingen, handleiding, etcetera.

Eigen aanbod

Zet uw eigen aanbod op een rij:

- Welke cursussen organiseert uw Bibliotheek?
- Welke spreekuren organiseert uw Bibliotheek?
- Andere verwante activiteiten?

Aandachtspunt: Kunnen de medewerkers geïnteresseerden meteen inschrijven voor een cursus?

Resultaat

Maak een duidelijk overzicht van het aanbod van de Bibliotheek, met locatie, datum, tijd, prijs en een uitleg van wat men kan halen en leren. Gebruik eenvoudige taal en vermijd woorden die de potentiële klanten niets zeggen (mediawijsheid, Digisterker, e-overheid etcetera).

- Presenteer het als samenhangend geheel.
- Zorg voor flyers en posters.
- Zorg dat het overzicht op een centrale plek te vinden is voor de frontoffice-medewerkers.

Tip

Bekijk na de inventarisatie voor de sociale kaart, waar er in het vangnet nog gaten zitten. Wellicht kan de Bibliotheek hier een aanbod voor samenstellen, of in overleg laten organiseren door één van de netwerkpartners.

Techniek en inrichting

De ervaring leert dat niet alle medewerkers op de hoogte zijn van de werkwijze van de publieks- en personeelspc's. Ook blijken publiekspc's niet altijd te werken conform de afspraken. Hierdoor kunnen klanten soms gegevens van hun voorgangers zien, kunnen documenten verloren gaan en andere ongewenste situaties zich voordoen. Dit heeft al tot hooglopende discussies met klanten geleid, met zelfs schadeclaims en (dreigen met) rechtszaken. Het is daarom goed om een aantal zaken te inventariseren.

Publiekswerkplekken; techniek

- Controleer met de ICT-aanbieder of de werking van de publiekspc's werkelijk overeenkomt met de afspraken. Denk aan zaken als:
 - Wat gebeurt er met de bestanden van de gebruiker als hij uitlogt.
 - Wanneer worden persoonlijke bestanden van het systeem gewist.
 - Kan een gebruiker zelf bestanden wissen.
 - Zijn er plekken op het systeem (bijvoorbeeld de server) waar persoonlijke bestanden staan.
 - Wat gebeurt er als een gebruiker niet uitlogt uit zijn account (webmail, Facebook etcetera). Kan de volgende klant dan in het account van de vorige gebruiker komen?
- Zorg dat het besturingssysteem, de software en beveiliging up-to-date zijn. Dit is een inspanningsverplichting die de Bibliotheek heeft in haar dienstverlening (het aanbieden van de werkplekken).
- Wordt er gebruikgemaakt van open wifi, of moeten bezoekers eerst inloggen?
- Controleer of de technische infrastructuur voldoet aan de eisen die de Belastingdienst stelt aan bibliotheken die met het convenant aan de slag gaan.
- Check of de medewerkers de publiekspc's monitoren.
 - Is dit bekendgemaakt aan het publiek? Dit is wettelijk verplicht.
 - Is het personeel op de hoogte van de voorwaarden waaronder monitoring mag plaatsvinden?
- Stel gebruiksregels op voor het aanbieden van computer- en internetfaciliteiten.
 - Onder welke voorwaarden mag een bibliotheekbezoeker gebruikmaken van de computer- en internetfaciliteiten? Denk aan prijs, tijdsduur, wel of geen pas nodig, printen, scannen, etcetera.
 - Wat mag de gebruiker wel en wat niet? Denk aan faciliteiten en gedrag.
 - Wordt er gefilterd?
 - Etcetera.

Resultaat

- Beschrijf de werking van het systeem voor de frontoffice-medewerkers, zorg dat dit bij hen bekend is en stel de beschrijving centraal aan hen beschikbaar.
- Beschrijf de werking van het systeem voor de bibliotheekbezoekers (zie ook Communicatie).

Publiekswerkplekken; inrichting en privacy

In de bibliotheekpraktijk is het een lastig dilemma: kies je voor afgeschermd werkplekken of voor overzicht en controle? Beide scenario's hebben voordelen, maar ook sterke nadelen. Met overzicht is het computergebruik beter in de gaten te houden en kunt u ingrijpen als klanten overlast bezorgen. Dit overzicht beperkt u door klanten meer privacy te bieden. Daarentegen is meer privacy veiliger voor klanten die de publiekswerkplekken gebruiken om persoonlijke en financiële zaken te regelen. Zeker nu klanten actief worden gewezen op de mogelijkheid om belastingaangifte te doen in de Bibliotheek, is het noodzakelijk om hiervoor goede faciliteiten te bieden.

Aandachtspunten hierbij zijn:

- Overweeg de inrichting van meerdere werkplekken waar klanten privacygevoelige computerzaken kunnen doen, zonder dat anderen makkelijk kunnen meekijken.
- Overweeg de overige werkplekken beter te beschermen tegen meekijken. Zijn daar simpele oplossingen voor te bedenken? Denk bijvoorbeeld aan:
 - Een schot tussen de werkplekken.
 - Voorzetschermen voor het beeldscherm die de inblikhoek verminderen.
- Controleer of klanten veilig kunnen pinnen op het betaalstation zonder dat er mensen meekijken. Bijvoorbeeld door een streep voor wachtenden aan te brengen.

- Controleer of de printers, scanners en kopieerapparaten zo staan dat niet iedereen er zo maar bij kan.
 - Moet de klant van de werkplek weglopen om een print op te halen? En zo ja: hoe ver liggen werkplek en printer van elkaar?
 - Komt de print meteen uit de printer, of moet de klant op een betaalstation of de printer eerst een handeling uitvoeren?
 - Hoe groot is het risico dat prints van verschillende klanten door elkaar uit de printer komen?
 - Is er tussenkomst van een medewerker vereist voordat een klant een print kan ophalen?

Resultaat

Een bewuste afweging van de inrichting van de werkplekken.

Personeelswerkplekken

- Communiceer duidelijk naar de frontoffice-medewerkers hoe zij moeten handelen achter de personeelswerkplekken.
 - Moet de medewerker het scherm zelf vergrendelen? Hoe?
 - Moet de medewerker het scherm zelf op de startpagina van het bibliotheek-automatiseringssysteem zetten?
 - Wordt het scherm automatisch vergrendeld? Hoe lang duurt het voordat het scherm wordt vergrendeld?
 - Mag de medewerker documenten van klanten (van USB-sticks, geheugenkaarten en dergelijke) openen op de personeelspc's?
 - Hoe moet de medewerker klanten helpen met privacygevoelige en financiële vragen?
 - Met gedempt volume praten.
 - Naar een aparte ruimte gaan.
 - Een streep op de vloer waar de andere klanten achter dienen te staan.

Resultaat

De medewerkers worden zich bewust van de wijze waarop zij de privacy van klanten waarborgen. Kennis en gedrag worden afgestemd, zodat alle medewerkers over dezelfde kennis beschikken en op dezelfde wijze werken.

Tip

Besteed tijdens werkoverleggen regelmatig aandacht aan de wijze waarop het personeel omgaat met de privacy van klanten. Verzamel ervaringen en cases om met elkaar te bespreken, afspraken te toetsen en privacy top of mind te houden.

Communicatie

Uw organisatie heeft op basis van het voorgaande haar beleid duidelijk geformuleerd en uw medewerkers weten hoe zij moeten handelen. Nu moeten de bibliotheekbezoekers kennis kunnen nemen van de manier waarop de Bibliotheek met hun privacy omgaat. Enerzijds om verwachtingen te kunnen managen en duidelijk uit te leggen waar de Bibliotheek voor staat. Anderzijds om op terug te kunnen vallen als er problemen ontstaan.

Aandachtspunten zijn:

- Bepaal de plekken waar gecommuniceerd wordt. Te denken valt aan:
 - De ingang
 - De balie: een bordje en/of een folder, waarin privacy-kwesties en computerregels worden uitgelegd, met een verwijzing naar het volledige reglement op papier en de website.
 - De website: het complete reglement.
 - Bij de computerwerkplek: een bordje en/of folder met verwijzing naar het volledige reglement.
 - Op het beginscherm van de publiekwerkplekken: klanten dienen eerst akkoord te gaan met de voorwaarden, voordat ze gebruik kunnen maken van de computer.
 - Op het beginscherm van het wifi-inlogscherm: klanten dienen eerst akkoord te gaan met de voorwaarden, voordat ze gebruik kunnen maken van de wifi.
 - Huishoudelijk reglement en andere relevante communicatie-uitingen voor klanten: integreer het privacyreglement hierin of verwijs ernaar.
- Communiceer duidelijk de gebruiksregels van de publiekscomputers en wat de klant mag verwachten aan hulp. De inhoud kan bestaan uit:
 - Welk niveau van dienstverlening mag een klant verwachten van de Bibliotheek.
 - De Bibliotheek kan niet garanderen dat de publiekspc's, het netwerk en de printfaciliteiten altijd goed functioneren.
 - Besteed aandacht aan de bewustwording van de klant als het gaat om zijn privacy.
 - Gebruiksregels voor internetvoorzieningen.
 - Het gebruikmaken van computer- en internetvoorzieningen is voor eigen risico.
 - De eindverantwoordelijkheid voor het gebruik van de dienstverlening ligt bij de klant.
- Verplicht u tot niet meer dan u waar kunt maken. Maak duidelijk dat alle verplichtingen rond de computer- en internetvoorzieningen louter inspannings- en geen resultaatverbintenissen zijn. De Bibliotheek kan niet garanderen dat de service voortdurend beschikbaar is en geschikt is voor normaal gebruik. Het gaat om verwachtingsmanagement op het niveau van verplichtingen, niet (primair) op het niveau van aansprakelijkheid.
- Bepaal met elkaar welke boodschap de frontoffice-medewerker aan de klant vertelt. Formuleer in begrijpelijke en eenvoudige bewoordingen wat het beleid van de Bibliotheek is, tot hoe ver de dienstverlening strekt en wat de klant mag verwachten van de Bibliotheek, en wat niet. Doe dit desnoods aan de hand van voorbeeldzinnen.

Resultaat

Het personeel communiceert dezelfde boodschap en klanten weten wat zij wel en niet mogen verwachten van de dienstverlening van de Bibliotheek.

Kennis

- Organiseer bijeenkomsten met het frontofficepersoneel. Behandel daarin:
 - Het begrip privacy.
 - Het beleid van de Bibliotheek.
 - Bespreek vooral veel cases en ga in op de ervaring van het personeel.
 - Houding en gedrag van het personeel.
 - Ondersteuning van de Bibliotheek aan het personeel.
 - Tips en uitleg over het computergebruik.
 - Vraag wat er mist aan ondersteuning en kennis.
 - Laat het onderwerp regelmatig terugkeren tijdens werkoverleggen en behandel ervaringen uit de praktijk. Is het protocol nog steeds voldoende of dient het aangepast te worden aan nieuwe situaties?

Overig

- Controleer of de verzekering up-to-date is en aansluit bij het huidige niveau van dienstverlening. Dit is belangrijk omdat computer- en internetfaciliteiten aanbieden en klanten helpen bij privacygevoelige en financiële vragen risico's met zich mee kan brengen.
- Controleer of de geheimhoudingsplicht voor privacygevoelige persoonsgegevens is opgenomen in de arbeidscontracten van uw medewerkers. Hierbij kan volstaan worden met de verwijzing in het arbeidscontract naar de cao waarin dit opgenomen is. Hoofdstuk VIII, artikel 53